JOURNAL OF ALGEBRA **124**, 493–505 (1989)

Problems Equivalent to Rational Diophantine Solvability[1]

K. H. KIM AND F. W. ROUSH

Mathematics Research Group, Alabama State University, Montgomery, Alabama 36195

Communicated by Walter Feit

Received August 5, 1987

Under the hypothesis that rational Diophantine equations are unsolvable we classify a number of other problems as solvable or unsolvable, such as $gV \subset hW$ for $g \in G$, $h \in H$ algebraic groups, V, W subspaces, existence of monomorphisms and epimorphisms of modules and algebras, existence of submodules of various types.

1. INTRODUCTION

In 1970, Matijasevich [11] added the final and long sought element to the efforts of Davis, Putman, and Robinson [4] to prove the unsolvability by any general algorithm of Diophantine equations, i.e., polynomials in n variables over $\mathbf{Z}$ (and $\mathbf{Z}^+$). Here we consider the consequences of the hypothesis.

$\mathscr{R}_d$: *There is no algorithm which decides for any n variable polynomial P over* $\mathbf{Q}$, *whether P has a solution in* $\mathbf{Q}$.

In the integer case, Jones [7] gives an example of a universal unsolvable equation, i.e., a polynomial in $a, x_1, ..., x_n$ such that there is no algorithm deciding for each a, existence of a solution $x_1, ..., x_n$.

We show that an arbitrary rational Diophantine equation can be cast into many forms, such as determinants, homogeneous systems, and so on and in this way we prove a number of algebraic problems are unsolvable under $\mathscr{R}_d$.

Diophantine equations in general are discussed in [3, 10, 12]. Major positive results appear in [2, 5, 6, 13, 14]. The present work is an outgrowth of problems in [8, 9].

Algorithmic unsolvability of a class of equations means that there is no recursieve algorithm for solving them; equivalently, that no Turing

[1] Partially supported by NSF DMS-8521533.

0021-8693/89 $3.00

machine exists which given the parameters specifying a member α of the class, in a finite number of steps prints zero if α has no solution and 1 if α has a solution. All Diophantine unsolvability results depend ultimately on a reduction to the halting problem for Turing machines.

Here we treat the following module problems for finitely generated modules over finitely additively generated $\mathbf{Q}$ algebras, specified by basis and products of basis elements:

(1) *Is there an epimorphism* $\mathcal{M} \to \mathcal{N}$?

(2) *Is there an monomorphism* $\mathcal{M} \to \mathcal{N}$?

(3) *Can we find a composition series for* $\mathcal{M}$?

(4) *Can we split* $\mathcal{M}$ *into indecomposable summands*?

(5) *Can we determine if* $\mathcal{M}$ *has a k-dimensional submodule*?

(6) *Can we determine the orders in which composition factors can occur*?

(7) *Can we determine if* $\mathcal{M}$ *is a direct summand of* $\mathcal{N}$?

We call (1)–(7) respectively the *epimorphism*, *monomorphism*, *composition series*, *decomposability*, *dimension*, *composition factors*, and *summand problems*. We also deal with (1), (2) for algebras and with commutative and Lie and study group problems of the form: Do there exist $g \in G$, $h \in H$, $\rho(g)V \subset \gamma(h)W$ for subspaces V, W and representations ρ, γ of algebraic groups G, H? We show that the existence of square roots in general finite dimensional algebras is unsolvable.

All undecidability results here assume $\mathcal{R}_d$. It follows from Matijasevich's result or Jones' explicit form that polynomials of some fixed degree in a given number of variables are unsolvable, but we do not assume this in the rational case.

2. Group Problems

Grunewald and Segal [5] proved that it is indecidable for an algebraic group G over $\mathbf{Z}$, an integer representation ρ of z, and an integer vector v and a subspace (kernel of a set of linear equations) W whether $gv \in W$ for some g. Their proof goes directly over to the rational case.

Proposition 2.1. *Under* $\mathcal{R}_d$ *it is unsolvable whether for* $n \in \mathbf{Z}^+$, *a rational representation* ρ *of* $GL(n, \mathbf{Q})$, *a vector* v, *and a subspace* W *there exists* $g \in GL(n, \mathbf{Q})$ *such that* $\rho(g)\, v \in W$.

Proof. Let the representation be the direct sum of all tensor powers of the standard representation up to the nth. Let the vector be the direct sum

of $(1, 0, ..., 0)$. Then vg has entries all monomials of degree at most n in the top row of G, which can be any nonzero vector. Then the subspace W can specify any relation in the monomials, i.e., any polynomial.

Under $\mathscr{R}_d$ it is undecidable if a nonzero solution exists of polynomials, since we can take $p(x_1 - x_2, x_3, ..., x_n)$. ∎

Most algebraic structure problems are stated naturally by homogeneous Diophantine equations.

$\mathscr{R}_h$: There exists no algorithm to decide whether a homogeneous Diophantine equation over $\mathbf{Q}$ has a solution other than $(0, ..., 0)$.

It is a folk theorem that $\mathscr{R}_d \Leftrightarrow \mathscr{R}_h$.

THEOREM 2.2. $\mathscr{R}_h \Leftrightarrow \mathscr{R}_d$.

For the record, we give an observation supplied by the referee, as basis for a proof of this well-known result. An equation $p(u_1, ..., u_n) = 0$ and $t \neq 0$ are equivalent to existence of $x_1, ..., x_4, y_1, ..., y_4$ such that $p(u_1, ..., u_n) = 0$ and $(u_1^2 + \cdots + u_n^2 + x_1^2 + \cdots + x_4^2)^2 - 3(y_1^2 + \cdots + y_4^2)^2 = t^4$, where not all variables are zero.

THEOREM 2.3 (Adler [1]). *Under $\mathscr{R}_d$ systems of the form*

$$\sum a_{ijk} x_i y_j = 0$$

with not all $x_i = 0$, not all $y_i = 0$ are unsolvable. Moreover, we can require that if a solution exists one exists with both x, y n-vectors for some $n \in \mathbf{Z}^+$ and for $i = 1, ..., n$, $x_i > 0$ and $x_i = y_i$.

THEOREM 2.4. *It is unsolvable under $\mathscr{R}_d$ given conjugate linear groups X, Y of diagonal matrices and D a linear space of matrices whether there exists $x \in X$, $y \in Y$ with $xy \in D$?*

Proof. By Theorem 2.3 systems of the form

$$\sum a_{ijk} x_i y_j = 0,$$

all $x_i, y_i \neq 0$ are unsolvable, where x, y are n-vectors for some n. Let X, Y be diagonal matrices made up of x_i, y_i arranged so as to give all products $x_i y_j$. Then linear combinations of these (a subspace) give the equations. ∎

COROLLARY. *$y \in x^{-1}D$ is unsolvable.*

COROLLARY. *For a commutative group G acting quadratically $Gv \subset W$ is unsolvable, in the situation of Proposition* 2.1.

THEOREM 2.5. *Under $\mathscr{R}_d$ it is unsolvable given invertible B, a subspace H, and m, $n \in \mathbf{Z}^+$ if there exist X, Y such that $XBY \in H$ and X, Y are $n \times n$ block diagonal invertible matrices each with identical blocks, i.e., $X = X\langle 0\rangle \oplus \cdots \oplus X\langle 0\rangle$, $Y = Y\langle 0\rangle \oplus \cdots \oplus Y\langle 0\rangle$ with $X\langle 0\rangle$, $Y\langle 0\rangle \in GL(m, \mathbf{Q})$.*

Proof. Under $\mathscr{R}_d$ there exist equations

$$\sum a_{ijk} x_j y_k = 0$$

such that it is undecidable if a solution exists with all $x_k \neq 0$, all $y_k \neq 0$.

First we show the theorem is true for noninvertible B.

Let $B\langle 0\rangle$ have (1, 1)-entry 1 and all other entries 0, and let B be a sum $B\langle 0\rangle \oplus \cdots \oplus B\langle 0\rangle$ corresponding to the sums for X, Y. Then $X\langle 0\rangle\, B\langle 0\rangle\, Y\langle 0\rangle$ is a matrix of all products from column 1 of $X\langle 0\rangle$ and row 1 of $Y\langle 0\rangle$. If the first row and column of $Y\langle 0\rangle$, $X\langle 0\rangle$ respectively are nonzero we can extend to invertible matrices. Let x_i, y_j be the entries in the first column of X, row of Y.

All equations $\sum a_{ijk} x_i y_j$ give linear spaces of $m \times m$ matrices for each $X\langle 0\rangle\, B\langle 0\rangle\, Y\langle 0\rangle$. By direct sum we obtain any system of equations. So the problem is unsolvable.

Now to replace $B\langle 0\rangle$ by invertible matrices write B as a difference $C\langle 1\rangle - C\langle 2\rangle$ of invertible matrices. Then any $XBY \in H$ is equivalent to

$$\begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} C\langle 1\rangle & 0 \\ 0 & C\langle 2\rangle \end{bmatrix} \begin{bmatrix} Y & 0 \\ 0 & Y \end{bmatrix} \varepsilon \left\{ \begin{bmatrix} M & 0 \\ 0 & N \end{bmatrix} : M - N \in H \right\}. \quad \blacksquare$$

THEOREM 2.6. *Under $\mathscr{R}_d$ it is undecidable whether for G, H linear groups acting on a vector space and V_0, V, W subspace of V_0 there exist $g \in G$, $h \in H$ such that $gV = hW$.*

Proof. Take the unsolvable problem of Theorem 2.4 written as $gV_1 \subset hW_1$, $g \in G_1$, $h \in H_1$ where V_1 is the 1 dimensional vector subspace of a total space U_1 spanned by an identity matrix I, h is x^{-1}, W_1 is D. Let $V_0 = U_1 \oplus U_2$ where $\dim(U_2) = \dim(W_1 - 1)$. We require that U_1 be an invariant subspace of G and U_2 an invariant subspace of H with the previous actions on U_1, as subspace and quotient space. Let $W = W_1$, $V = V_1 \oplus U_2$.

Then $gV_1 \subset hW_1$ for $g \in G$, $h \in H_1$ is necessary in order that $gV = hW$ since $gV_1 \subset gV = hW$. And $hW/U_2 = h(W_1)$.

Let the groups G, H be the sets of all linear transformations of V_0 keeping U_1, U_2 respectively invariant having the given actions on U_1 as submodule and quotient module. Suppose $gV_1 \subset hW_1$ is solvable. Write $hW_1 = gV_1 \oplus W_3 \subset U_1$. Multiply h by a map h_1 which is the identity on

the quotient by U_2 and on gV_1 and which sends W_3 into $W_3 \oplus U_2$ by (x, x) under some isomorphism $W_3 \to U_2$.

Multiply g by a map g_1 which is the identity on U_1 and maps $U_2 \to W_3 \oplus U_2$ by (x, x). Then $g_1 gV = h_1 hW$ is valid. ∎

THEOREM 2.7. *Suppose e are given algebraic groups G, H, subspaces V, W. Then the problem, do there exist $g \in G$, $h \in H$ such that $gV \subset hW$ has the following status:*

		General case	$V = W$	$\dim(V) = 1$	$\dim(V) = \dim(W) = 1$
G, H arbitrary algebraic groups	$H = \{e\}$	*U*	*S*	*U*	*S*
	any H	*U*	*U*	*U*	*U*
G, H defined by linear equations	$H = \{e\}$	*S*	*S*	*S*	*S*
	any H	*U*	*U*	*U*	*S*

Here S is solvable, U unsolvable.

Proof. Squares (1, 2) (1, 4) are solvable by Sarkisian [13] (he states [15] he has corrected the need for strong approximation). Square (1, 2) reduces to square (1, 4) on tensor powers. Squares (1, 1), (1, 3) are undecidable by Proposition 2.1.

Square (2, 4) follows from Proposition 2.1 since the nonzero elements of any subspace is Hv. Square (4, 3) is undecidable by the Corollary to Theorem 2.4. Square (4, 2) is undecidable by Theorem 2.6. This implies by containment all undecidable squares. Row 3 and square (4, 3) can be stated as linear equations subject to which G, H have rank n. This can be solved by seeing if determinants on this spaces are zero identically. ∎

3. SOLVABLE MODULE PROBLEMS

THEOREM 3.1. *The monomorphism, epimorphism, and split monomorphism problems are solvable.*

Proof. Each of these problems can be written as a set of inequations in rational variables, that is, a linear transformation, which has maximal rank. This means at least one of a set of determinants is not identically zero. The epimorphism problem is dual to the monomorphism.

The split monomorphism problem is, do f, g exist, where

$$\mathcal{N} \xrightarrow{f} \mathcal{M} \xrightarrow{g} \mathcal{N},$$

such that fg is an isomorphism. Take as variables coefficients in a vector space basis for all module homomorphisms $\mathcal{N} \to \mathcal{M}$ and $\mathcal{M} \to \mathcal{N}$. Then the condition is $\det(fg) \neq 0$. The monomorphism problem is similar. ∎

THEOREM 3.2. *For any finite dimensional module $\mathcal{M}$ over a finite dimensional algebra $\mathfrak{A}$, it is possible to find a composition series $\mathcal{M}_i$ (submodules $\mathcal{M}_i \subset \mathcal{M}_{i-1}$ such that $\mathcal{M}_{i-1}/\mathcal{M}_i$ is irreducible for each i).*

Proof. It suffices to find a proper nonzero irreducible submodule if one exists. This can be done by [8]. ∎

THEOREM 3.3. *It is possible to decompose $\mathcal{M}$ into summands which cannot be further decomposed.*

Proof. It is enough to find a proper nonzero summand of $\mathcal{M}$. A summand of $\mathcal{M}$ corresponds to an idempotent other than 0, I of $\mathrm{End}(\mathcal{M})$. Such an idempotent will give one in $\mathrm{End}(\mathcal{M})/\mathfrak{J}$, $\mathfrak{J}$ the Jacobson radical.

We can determine if such exists by [8]. Given an idempotent E of $\mathrm{End}(\mathcal{M})/\mathfrak{J}$, lift it to E in $\mathrm{End}(\mathcal{M})$. All eigenvalues of the lifting are 0, 1 by considering action on $\mathfrak{J}^n/\mathfrak{J}^{n+1}$. Therefore, some polynomial in the matrix E is idempotent of equal eigenvalues. ∎

4. UNSOLVABLE MODULE PROBLEMS

LEMMA 4.1. *Under $\mathcal{R}_d$, given array a it is unsolvable whether vectors x, y, z exist such that x, $y \neq 0$ and*

$$y_i z_j = \sum a_{ijp} x_p.$$

Proof. These equations amount to an arbitrary linear system on $y_i z_j$. If a_{ijp} is a 1–1 transformation x will be nonzero if and only if $y_i z_j$ is. So we get an arbitrary homogeneous system

$$\sum \beta_{ijp} y_i z_j = 0.$$

To make the mapping 1–1 in x, let x be coefficients in a basis for the required space of matrices spanned by $A\langle p \rangle$. ∎

THEOREM 4.2. *Let $\mathcal{M}$, $\mathcal{N}$ be irreducible modules over a finite dimensional algebra. Let $\mathfrak{A}$ be an extension of a direct sum of copies of $\mathcal{N}$ by a direct sum of copies of $\mathcal{M}$. Then it is undecidable if there is a submodule of form $\mathcal{N}$ extended by $\mathcal{M}$. We take the algebra to act on $\mathcal{M}$, $\mathcal{N}$ as full matrix algebras of arbitrary different dimensions. We may assume submodules $\mathcal{M}$ extended by $\mathcal{N}$ do not exist.*

Proof. Let the matrices specifying the module action on $\mathfrak{A}$ have the block fora (A_{rs}). In the upper left and lower right A_{rs} is block diagonal with diagonal entries equal to some matrices D, E. In upper right we have zero. There are a family of such matrices $A\langle p\rangle$, ranging over generators of the algebra. We also consider a large 2×2 block structure in which all $\mathscr{M}$'s additively are grouped together as block 1 and all $\mathscr{N}$'s as block 2.

Let the module action on the proposed submodule be given by D, E in the (1, 1)- and (2, 2)-blocks, zero in the upper right and X (unknown) in lower left. All these are indexed on p.

If a module homomorphism exists then on the diagonal blocks D, E it is multiplication by constants r_i, s_i. Let modules acting on the left and the module homomorphism be given by a matrix W, so that the conditions are

$$W\begin{bmatrix} D & 0 \\ X & E \end{bmatrix} = AW,$$

where W is 1–1 on main diagonal blocks, not all r_i are zero, and not all s_i are zero. W is not indexed on p. Its (2, 1)-block is subdivided into blocks W_i.

These give equations for each i, p (A_{ij} in the big (2, 1)-block)

$$W_i D + s_i X = \sum A_{ij} r_j + E W_i.$$

Let the matrices D, E for $p \neq 1, 2, 3, 4$ be zero. Let $D\langle 1\rangle$, $D\langle 2\rangle$ generate a full matrix algebra and $E\langle 3\rangle$, $E\langle 4\rangle$ generate a full matrix algebra. Let $A_{ijp} = D\langle 3\rangle = D\langle 4\rangle = E\langle 1\rangle = E\langle 2\rangle = 0$, $p = 1, 2, 3, 4$. Choose $W_i = s_i C$, $X = EC - CD$. This solves the equations for $p = 1, 2, 3, 4$, where $X = X\langle p\rangle$ varies with p.

Then the remaining system for $p > 4$ is

$$s_i X\langle p\rangle = \sum_j A_{ij}\langle p\rangle r_j.$$

Let the $A_{ij}\langle p\rangle$ be scalar multiples $a_{ijp}F$ of a fixed matrix. Then $X\langle p\rangle$ must be also $x_p F$. And

$$s_i x_p = \sum a_{ijp} r_j$$

where not all r, s are zero. This is unsolvable by Lemma 4.1.

In this situation it is not possible to reverse the composition factors in the submodule. If it were then the submodule would have a submodule $\mathscr{M}$ and be $\mathscr{M} \oplus \mathscr{N}$. Then in the equations above $X = 0$. But in Lemma 4.1 $A_{ij}\langle p\rangle$ were 1–1 so $x\langle p\rangle \neq 0$. ∎

COROLLARY. *The composition factors and dimension problems are unsolvable.*

5. UNSOLVABLE VECTOR SPACE PROBLEMS

THEOREM 5.1. *The problem of whether a linear space of matrices contains a singular matrix is unsolvable.*

Proof. Let $f=0$ a homogeneous Diophantine equation in $x_1, ..., x_n$.

Let M be an n-square linear matrix in x_i such that $\det(M)=0$ if and only if all $x_i=0$ over $\mathbf{Q}$. Take M from the regular representation of a degree n algebraic number field $\mathfrak{F}$ over $\mathbf{Q}$. Then $f^n(\det(M))^n=0$ is unsolvable.

We start with a 1×1 matrix $[f^n]$ and expand. First replace f^n by fI where I is an n-square identity matrix.

From here on let all matrices be in n-square blocks, each block corresponding to an element of $\mathfrak{F}$. Let t denote the block M. Its determinant is $\det(M)$. Determinants over $\mathbf{Q}$ are norms of $\mathfrak{F}$ determinants.

Change

$$\begin{bmatrix} a+b & * \\ * & * \end{bmatrix}$$

into

$$\begin{bmatrix} t & 0 & 0 \\ -a & a+b & * \\ 0 & * & * \end{bmatrix}$$

by a column operation into

$$\begin{bmatrix} t & t & 0 \\ -a & b & * \\ 0 & * & * \end{bmatrix}$$

This breaks up all sums and multiplies determinants by powers of t. It preserves homogeneity.

To deal with products, change

$$\begin{bmatrix} ab & * \\ * & * \end{bmatrix}$$

into

$$\begin{bmatrix} t & 0 & 0 \\ at & ab & * \\ 0 & * & * \end{bmatrix}$$

into

$$\begin{bmatrix} t & -b & 0 \\ at & 0 & * \\ * & * & * \end{bmatrix}$$

Now all products are a single variable times powers of t, and each row has constant degree. Now factor out a power of t from each row to make it linear. ∎

THEOREM 5.2. *Given coefficients β_{ijk} and $n_0 \in \mathbf{Z}^+$, homogeneous quadratic systems*

$$\sum \beta_{ijk} x_i y_j = 0 \tag{5.1}$$

of the following type are unsolvable for nonzero x, y, n_0 tuples of rational numbers:

(1) $y_i \sum_i \beta_{ik} x_i = 0$, $k = 1, ..., k_0$;

(2) $x_i y_j - x_r y_s = 0$, $(i, j, r, s) \in V$, *a given set of* 4 *tuples*;

(3) $x_i y_j - x_j y_i = 0$ *for all* $i, j = 1, ..., n_0$

where these are precisely the equations of the system.

Proof. Start with a homogeneous system (5.1) such that if a nonzero solution exists one exists with all variables nonzero. We introduce new variables x_{ij} with $x_{ij} = x_i x_j$ understood. Add equations $x_{ij} x_{rs} = x_{uv} x_{pm}$ whenever $uvpm$ is a permutation of $ijrs$. Now replace $\sum b_{ijk} x_i x_j$ by $x_{rs} \sum b_{ijk} x_{ij} = 0$. Here x_{rs} ranges over all variables. If a solution of the original exists with all x_i, $y_j \neq 0$ we have a solution of the new. If we have a nonzero solution of the new we can write $k x_{ij} = x_i x_j$ for some nonzero k by $x_{ij} x_{rs} = x_{uv} x_{pm}$. (So (x_{ij}) is rank 1.) This gives a nonzero solution of the old. ∎

THEOREM 5.3. *It is in general unsolvable whether a $2 \times n$ matrix X of rank 2 exists satisfying*

$$\det([X]\, A\langle i \rangle) = 0.$$

where $A\langle i \rangle$ are given $n \times 2$ matrices.

Proof. Such systems have the form

$$\det \begin{bmatrix} p(a) & r(a) \\ p(b) & r(b) \end{bmatrix},$$

where a, b are rows 1, 2 of X, p, r are any linear functions. These equations include

$$\begin{cases} a_{2i}b_{2j} - a_{2j}b_{2i} = 0 \\ a_{2i-1}b_{2j-1} - b_{2i-1}a_{2j-1} = 0 \end{cases}$$

which guarantee for some c_1, d_1, c_2, d_2, $a_{2i} = x_i c_2$, $b_{2i} = x_i d_2$, $a_{2i\ 1} = y_i c_1$, $b_{2i-1} = y_i d_1$. The matrix X has rank 2 if $x \neq 0$, $y \neq 0$, $c_1 d_2 - c_2 d_1 \neq 0$. Assume this. Then the equations have the form

$$\det \begin{bmatrix} p_1(x)c_1 + p_2(y)c_2 & r_1(x)c_1 + r_2(y)c_2 \\ p_1(x)d_1 + p_2(y)d_2 & r_1(x)d_1 + r_2(y)d_2 \end{bmatrix} = 0.$$

This is

$$(c_1 d_2 - c_2 d_1)(p_1(x)\, r_2(y) - r_1(x)\, p_2(y)) = 0.$$

So it includes all equations

$$x_i\, y_j - x_r\, y_s = 0.$$

Moreover, it includes all

$$p_1(x)\, y_j = 0.$$

Therefore by the previous theorem these are unsolvable. ∎

COROLLARY. *Given subspaces U_i, it is undecidable if a rank 2 subspace V exists such that for each i:*

$$V \cap U_i \neq \{0\}.$$

6. UNSOLVABLE RING PROBLEMS

THEOREM 6.1. *The monomorphism problem is unsolvable for two stage nilpotent finite dimensional commutative (or Lie) algebras under $\mathscr{R}_d$.*

Proof. Let R be a two stage nilpotent algebra additively isomorphic to $U \oplus V$ with product $(u, v)(x, y) = (0, \mathscr{B}(u, x))$ where $\mathscr{B}$ is a bilinear map. We can choose $\mathscr{B}$ so that the equation $\mathscr{B}(x, x)$ is an arbitrary homogeneous quadratic system so $\mathscr{B}(x, x) = 0$, $x \neq 0$ is unsolvable.

Let S be a zero ring isomorphic to $\mathbf{Q} \oplus V$ additively. Then a monomorphism $S \to R$ is equivalent to existence of nonzero x. For commutativity, replace $\mathscr{B}(x, y)$ by $\frac{1}{2}(\mathscr{B}(x, y) + \mathscr{B}(y, x))$. For Lie algebras, choose an antisymmetric bilinear form and let S be $\mathbf{Q} \oplus \mathbf{Q} \oplus V$ additively with zero products, using Theorem 5.3. ∎

THEOREM 6.2. *Existence of ring epimorphisms of commutative (or Lie) 2-step nilpotent algebras over* $\mathbf{Q}$ *is unsolvable under* $\mathscr{R}_{\mathscr{A}}$.

Proof. Consider 2-step nilpotent commutative algebras $\mathfrak{A}$, $\mathfrak{B}$ which additively are $U \oplus V$, $R \oplus S$ with products symmetric bilinear forms $\mathscr{B}_1$: $U \times U \to V$, $\mathscr{B}_2$: $R \times R \to S$. Assume $\mathscr{B}_2$ is nonsingular. Then an epimorphism must map V into S, as the kernel of xy over all y. Therefore we have a linear map h from V to S and an induced quotient map f from U to $R \oplus S/S \simeq R$. The latter map must be an epimorphism and

$$h(\mathscr{B}_1(x, y)) = \mathscr{B}_2(fx, fy)$$

for all x, y. Take bases for U, S and express the bilinear forms as $x\mathscr{B}_1\langle i \rangle y^T$, $x\mathscr{B}_2\langle i \rangle y^T$ projected to the respective basis elements. Then if f is given by a matrix F we have

$$\sum h_{ij} \mathscr{B}_1\langle j \rangle = F\mathscr{B}_2\langle i \rangle F,$$

where h_{ij} define the map h, for each i.

By Theorem 5.1, it is unsolvable whether a linear space L contains a nonsingular matrix. For any linear space L of matrices let $M\langle j \rangle$ be a basis and let

$$\mathscr{B}_1\langle j \rangle = \sum_{i=1}^{4} \begin{bmatrix} 0 & M\langle j \rangle^T \\ M\langle j \rangle & 0 \end{bmatrix}.$$

Any quadratic form

$$\bigoplus_{i=1}^{4} \begin{bmatrix} 0 & M^T \\ M & 0 \end{bmatrix}$$

will have Hasse invariant and discriminant trivial, since it is $h \oplus h \oplus h \oplus h$. Therefore, there are only a finite number of possibilities for its isomorphism type given by its rank and signature. Let $\mathscr{B}_1\langle j \rangle$ be $n \times n$.

If $\mathscr{B}_2$ is epic on $\mathbf{R} \otimes \mathbf{R}$ then h must be epic. Then any F, h_{ij} satisfying the above equations give an algebraic epimorphism.

Let $\dim(S) = 1$. Let $\mathscr{B}_2\langle 1 \rangle$ range over all representatives for a nonzero isomorphism type having rank less than n for finite set of algebras. If the

epimorphism of algebras problem were decidable then we could decide whether the matrix $\sum h_{ij} M\langle j\rangle$ in L is singular. This is false by Theorem 6.1.

The same construction with antisymmetric forms everywhere works for Lie algebras. There are no invariants except rank for antisymmetric bilinear forms. ∎

PROPOSITION 6.3. *It is unsolvable under $\mathscr{R}_d$ whether a linear space of quadratic forms from $\mathbf{Q}^n$ to $\mathbf{Q}$ contains a form isomorphic to a given quadratic form. The same holds for symmetric and antisymmetric bilinear forms.*

Proof. This follows from the last half of the proof above taking quadratic forms

$$\bigoplus_{i=1}^{4} \begin{bmatrix} 0 & M^T \\ M & 0 \end{bmatrix}. \quad \blacksquare$$

THEOREM 6.4. *In commutative nilpotent algebras, the equations*

$$xy = a, \qquad x^2 = a$$

are each not solvable under $\mathscr{R}_d$, given a.

Proof. Take as algebra for $x^2 = a$ a 2-step algebra $V \oplus W$ where $(x_i) \circ (y_j) = (\sum \beta_{ijk} x_i y_j)$ in component $\kappa > 1$ of a and is $x_1 y_1$ in component 1. Let $a = (1, 0, ..., 0)$. Then $x^2 = a$ if and only if $x_1^2 = 1$ $\sum \beta_{ijk} x_i x_j = 0$. We have seen this is unsolvable, in Theorem 2.3. Here β_{ijk} may be replaced by

$$\tfrac{1}{2}(\beta_{ijk} + \beta_{jik})$$

if it is not symmetric.

For $xy = a$, begin with such a symmetric β_{ijk} on variables x_i, $i = 1$ to n. Add variables y_i, z_i, w_i where y_i, z_i are to be x_i, w_i is to be $-x_i$. Take the same product together with new components $x_i y_i + z_i w_i$, $x_i w_j + z_j y_i$, to equal zero, where x_i, z_i make up x and y_i, w_i make up y. These equations are symmetric in x, y, and have a solution with $x_1 y_1 = 1$ if $\sum \beta_{ijk} x_i x_j$ has a positive solution.

Conversely, let x_1, $y_1 = 1$, $x_i y_i + z_i w_i = 0$, $x_i w_j + z_j y_i = 0$ for all i, j. Since $x_1 = y_1 = 1$, $z_1 w_1 = -1$, $z_1 + w_1 = 0$. So $z_1 = \pm 1$, $w_1 = -z_1$. By reversing signs of all z, w let $z_1 = 1$, $w_1 = -1$. Then $x_1 w_j + z_j y_1 = 0$ gives $w_j = -z_j$. And $x_i w_1 + z_1 y_i = 0$ gives $x_i = y_i$. Now $\sum \beta_{ijk} x_i y_j = 0$ is unsolvable. ∎

7. Conclusion

Many problems have a sharp boundary between the solvable and unsolvable under $\mathscr{R}_{\mathscr{A}}$, e.g., the composition series problem and the dimension problem, the problems $gV = hW$ versus $gV \subset hW$, epimorphisms and monomorphisms of modules versus algebras.

As an *open problem*, we leave: *given finite dimensional modules* $\mathscr{M}_1$, $\mathscr{M}_2$, $\mathscr{M}_3$ *is solvable whether a short exact sequence*

$$0 \to \mathscr{M}_1 \to \mathscr{M}_2 \to \mathscr{M}_3 \to 0$$

exists?

Acknowledgment

We thank the referee for useful criticism and background information.

References

1. A. Adler, A reduction of homogeneous Diophantine problems, *J. London Math. Soc.* **3** (1971), 446–448.
2. J. Ax, Solving Diophantine equations modulo every prime, *Ann. of Math.* **85** (1967), 161–187.
3. M. Davis, Y. Matijasevich, and J. Robinson, Hilbert's tenth problem Diophantine equations: positive aspects of negative solution, *Proc. Sympos. Pure Math.* **XXVIII** (1976), 223–378.
4. M. Davis, N. Putman, and J. Robinson, The decision problem for exponential Diophantine equations, *Ann. of Math.* **74** (1961), 425–436.
5. F. Grunewald and D. Segal, Some general algorithms I: Arithemetic groups, *Ann. of Math.* **112** (1980), 531–583.
6. F. Grunewald and D. Segal, Decision problems concerning S-arithmetic groups, *J. Symbolic Logic* **50** (1985), 734–772.
7. J. P. Jones, Undecidable Diophantine equations, *Bull. Amer. Math. Soc.* **3** (1980), 859–862.
8. K. H. Kim and F. W. Roush, Some results in decidability of shift equivalence, *J. Combin. Inform. System Sci.* **4** (1979), 123–146.
9. K. M. Kim and F. W. Roush, Decidability of shift equivalence, *in* "Proceedings of the Special Year in Dynamical Systems, University of Maryland, College Park, 1986," Lecture Notes in Mathematics No. 1342, Springer, Berlin, 1988.
10. S. Lang, Hyperbolic and Diophantine analysis, *Bull. Amer. Math. Soc.* **14** (1986), 159–205.
11. Y. Matijasevich, Enumerable sets are Diophantine, *Soviet Math. Dokl.* **11** (1970), 354–357.
12. B. Mazur, Arithmetic on curves, *Bull. Amer. Math. Soc.* **14** (1986), 207–267.
13. R. A. Sarkisian, Galois cohomology and some questions of the theory of algorithms," *Mat. Sb.* **39** (1981), 519–545.
14. R. A. Sarkisian, A problem of equality for Galois cohomology, *Algebra and Logic* **19** (1980), 459–472.
15. R. A. Sarkisian, personal correspondence.